AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) An automated method of preventing an endnode in a communication fabric from receiving an unauthorized communication, comprising:

establishing a first category of management communications to include:

a request from a manager node to an endnode; and

a reply from the manager node to a request from an endnode;

establishing a second category of management communications to include:

a reply from an endnode to a request from the manager node; and

a request from an endnode to the manager node; and

at a switching device coupled to a first endnode:

receiving from the communication fabric a management communication packet addressed to the first endnode;

determining whether the first endnode is a trusted endnode;

determining whether the management communication is a first category management communication based on ~~a management class~~ ~~of the node~~ whether the management communication is originated from a manager node and whether the management communication is a request or a reply; and

responsive to~~if~~ the first endnode not being ~~is not~~ a trusted endnode and the management communication not being a first category management communication,~~;~~ ~~-~~discarding the management communication ~~if the management communication is not a first category management communication~~.

2. (Original) The method of claim 1, further comprising:

classifying each endnode in the communication fabric as either trusted or untrusted.

3. (Original) The method of claim 2, wherein said classifying comprises:

associating with each port of the switching device an indicator configured to indicate whether a node coupled to the port is trusted.

4. (Original) The method of claim 2, wherein said classifying comprises:

classifying the first endnode as a trusted endnode if the first endnode is a manager node.

5. (Original) The method of claim 2, wherein said classifying comprises:

classifying the first endnode as an untrusted endnode if the first endnode is not configured to act as a manager node.

6. (Original) The method of claim 1, wherein said determining comprises:

reading an indicator associated with a port of the switch to which the first endnode is coupled;

wherein said indicator is configured to indicate whether the first endnode is trusted.

7. (Currently Amended) The method of claim 1, further comprising, at the switching device:

~~If~~responsive to the first endnode being a ~~is~~ trusted endnode, forwarding the management communication to the first endnode regardless of the category of the management communication.

8. (Currently Amended) The method of claim 1, further comprising, at the switching device:

receiving a second management communication from the first endnode; and

responsive to the management communication not being a second category management communication, discarding the second management communication~~ if the management communication is not a second category management communication~~.

9. (Original) The method of claim 1, wherein the communication fabric comprises a subnet of an InfiniBand communication fabric.

10. (Original) The method of claim 9, wherein a management communication comprises a communication transmitted on virtual lane 15 of the InfiniBand communication fabric.

11. (Currently Amended) A computer readable medium storing instructions that, when executed by a computer, cause the computer to perform a method of preventing an endnode in a communication fabric from receiving an unauthorized communication, comprising:

establishing a first category of management communications to include:

a request from a manager node to an endnode; and

a reply from the manager node to a request from an endnode;

establishing a second category of management communications to include:

a reply from an endnode to a request from the manager node; and

a request from an endnode to the manager node; and

at a switching device coupled to a first endnode:

receiving from the communication fabric a management communication addressed to the first endnode;

determining whether the first endnode is a trusted endnode;

determining whether the management communication is a first category management communication based on ~~a management class of the node~~whether the management communication is originated from a manager node and whether the management communication is a request or a reply; and

~~if~~responsive to the first endnode not being ~~is not~~ a trusted endnode and the management communication not being a first category management communication, discarding the management communication ~~if the management communication is not a first category management communication~~.

12. (Currently Amended) An automated method of preventing an endnode in a communication fabric from sending an unauthorized communication, comprising:

establishing a first category of management communications to include:

a request from a manager node to an endnode; and

a reply from the manager node to a request from an endnode;

establishing a second category of management communications to include:

a reply from an endnode to a request from the manager node; and

a request from an endnode to the manager node; and

at a switching device coupled to a first endnode:

receiving from a first endnode a management communication addressed to a second endnode in the communication fabric;

determining whether the first endnode is a trusted endnode;

determining whether the management communication is a second category management communication based on ~~a management class of the node~~whether the management communication is destined for~~originated from~~ a manager node and whether the management communication is a request or a reply; and

~~if~~responsive to the first endnode ~~is~~ not being a trusted endnode and the management communication not being a second category management communication, discarding the management communication~~ if the management communication is not a second category management communication~~.

13. (Original) The method of claim 12, further comprising:

classifying each endnode in the communication fabric as either trusted or untrusted.

14. (Original) The method of claim 12, wherein said classifying comprises:

associating with each port of the switching device an indicator configured to indicate whether a node coupled to the port is trusted.

15. (Currently Amended) The method of claim 12, wherein said classifying comprises:

responsive to the first endnode being a manager node, classifying the first endnode as a trusted endnode ~~if the first endnode is a manager node~~.

16. (Currently Amended) The method of claim 12, wherein said classifying comprises:

responsive to the first endnode not being configured to act as a manager node, classifying the first endnode as an untrusted endnode ~~if the first endnode is not configured to act as a manager node~~.

17. (Original) The method of claim 12, wherein said determining comprises:

reading an indicator associated with a port of the switch to which the first endnode is coupled;

wherein said indicator is configured to indicate whether the first endnode is trusted.

18. (Currently Amended) The method of claim 12, further comprising, at the switching device:

responsive to ~~if~~ the first endnode being a ~~is~~ trusted endnode, forwarding the management communication toward the second endnode regardless of the category of the management communication.

19. (Currently Amended) The method of claim 12, further comprising, at the switching device:

receiving a second management communication addressed to the first endnode; and responsive to the management communication not being a first category management communication, discarding the second management communication ~~if the management communication is not a first category management communication~~.

20. (Original) The method of claim 12, wherein the communication fabric comprises a subnet of an InfiniBand communication fabric.

21. (Original) The method of claim 20, wherein a management communication comprises a communication transmitted on virtual lane 15 of the InfiniBand communication fabric.

22. (Currently Amended) A computer readable medium storing instructions that, when executed by a computer, cause the computer to perform a method of preventing an endnode in a communication fabric from sending an unauthorized communication, comprising:

establishing a first category of management communications to include:

a request from a manager node to an endnode; and

a reply from the manager node to a request from an endnode;

establishing a second category of management communications to include:

a reply from an endnode to a request from the manager node; and

a request from an endnode to the manager node; and

at a switching device coupled to a first endnode:

receiving from a first endnode a management communication addressed to a second endnode in the communication fabric;

determining whether the first endnode is a trusted endnode;

determining whether the management communication is a second category management communication based on ~~a management class of the node~~whether the management communication is destined for~~originated from~~ a manager node and whether the management communication is a request or a reply; and

responsive to ~~if~~ the first endnode ~~is~~ not being a trusted endnode, discarding the management communication if the management communication is not a second category management communication.

23. (Currently Amended) An apparatus for preventing a node in a communication fabric from engaging in unauthorized communication, the apparatus comprising:

a switching device configured to route management communications through the communication fabric, wherein:

a type one management communications comprise requests from a manager node to endnodes and replies from the manager node to requests from endnodes; and

a type two management communications comprise replies from endnodes to requests from the manager node and requests from endnodes to the manager node;

wherein a management communication is categorized to be a type one or a type two management communication based on ~~a management class of the node~~ whether the management communication is originated from or destined for a manager node and whether the management communication is a request or a reply ;

for each port of the switching device, an indicator configured to indicate whether an endnode coupled to the port is trusted;

wherein a first management communication addressed to a first endnode coupled to a first port of the switching device is discarded responsive to the first endnode not being a trusted endnode and the first management communication not being a type one management communication ~~if the first endnode is not trusted and the first management communication is not a type one management communication~~; and

wherein a second management communication received from the first endnode is discarded responsive to ~~if~~ the first endnode ~~is~~ not being a trusted endnode and the second management communication ~~is~~ not being a type two management communication.

24. (Original) The apparatus of claim 23, further comprising:

a secure channel configured to allow a management node to configure said indicators.

25. (Original) The apparatus of claim 23, wherein:

for each port coupled to another switching element, said indicator is set to indicate the other switching element is trusted.

26. (Original) The apparatus of claim 23, wherein:

for each port coupled to a management node, said indicator is set to indicate the management node is trusted.

27. (Original) The apparatus of claim 23, wherein:

for each port coupled to an endnode that is not configured to act as a management node, said indicator is set to indicate the endnode is not trusted.

28. (Original) The apparatus of claim 23, wherein:

the communication fabric comprises an InfiniBand communication fabric; and a management communication comprises a communication transmitted over virtual lane 15 of the InfiniBand communication fabric.

29. (Currently Amended) A computer readable medium residing in a communication switch and containing a data structure configured for indicating trust, the data structure comprising:

for each port of the communication switch, an indicator configured to indicate whether a communication node coupled to the port is trusted;

wherein a port indicator is set to a first state responsive to ~~if~~the coupled communication node being a ~~is~~trusted node and is set to a second state responsive to ~~if~~the coupled communication node ~~is~~not being a trusted node; and

wherein management communications addressed to the coupled communication node are filtered based on ~~a management class of the node~~whether the management communication is originated from or destined to a manager node and whether the management communication is a request or a reply if the port indicator is set to said second state.